The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
12/14/2010
SUBJECT:
Multiple vulnerabilities in Microsoft Office Publisher Could Allow Remote Code Execution (MS10-103)

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft Publisher, which could allow an attacker to take complete control of an affected system. Microsoft Publisher, a component of Microsoft Office, is an application that allows users to create marketing materials and other types of publications. Exploitation may occur if a user opens a specially crafted Publisher file. This file may be received as an email attachment, or downloaded via the Web. Successful exploitation may result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Microsoft Office Publisher 2002
- Microsoft Office Publisher 2003
- Microsoft Office Publisher 2007
- Microsoft Office Publisher 2010

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:
Multiple vulnerabilities have been discovered in Microsoft Publisher, which could allow an attacker to take complete control of an affected system. These vulnerabilities may be exploited if a user visits, or is redirected to a web page; or opens a malicious file that was designed to take advantage of these vulnerabilities. These vulnerabilities may also be exploited if a user opens an email that has a specially crafted file designed to leverage these vulnerabilities. The vulnerabilities are as follows:

- Size Value Heap Corruption in pubconv.dll exists when a specially created Publisher files is parsed.
- A Heap Overrun vulnerability in pubconv.dll exists when a user opens a malicious file.
- A Memory Corruption vulnerability exists when a specially crafted Publisher 97 formatted file is parsed.
- A Memory Corruption vulnerability exists when a specially crafted Publisher file is parsed.
- Array Indexing Memory Corruption vulnerability exists when a specially crafted Publisher file is parsed.

Successful exploitation may result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.

REFERENCES:
Microsoft:
http://www.microsoft.com/technet/security/Bulletin/MS10-103.mspx

Security Focus:
http://www.securityfocus.com/bid/45282
http://www.securityfocus.com/bid/45279
http://www.securityfocus.com/bid/45277
http://www.securityfocus.com/bid/45280

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2569
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2570
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2571
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3954
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3955